Symantec

Sumário Executivo

Relatório de Ameaças à Segurança na Internet 2018

ISTR

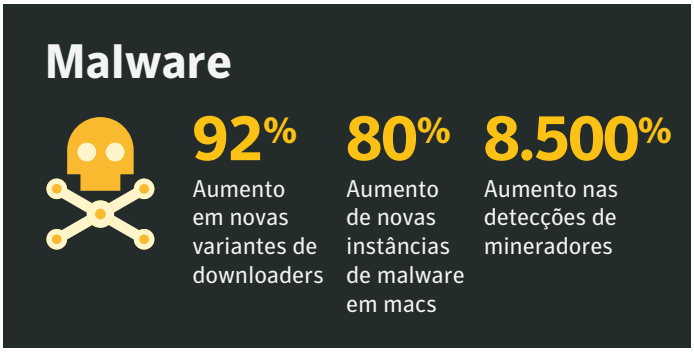
Volume 23

Sumário Executivo

Da propagação repentina do WannaCry e Petya/NotPetya ao rápido crescimento de mineradores de criptomoedas, 2017 nos proporcionou outro alerta, que as ameaças à segurança digital podem vir de fontes novas e inesperadas. A cada ano que passa, além do aumento do volume absoluto de ameaças, o cenário de ameaças se tornou mais diversificado, com um maior trabalho dos grupos de ataque para descobrir novos caminhos de ataques e encobrir seus rastros.

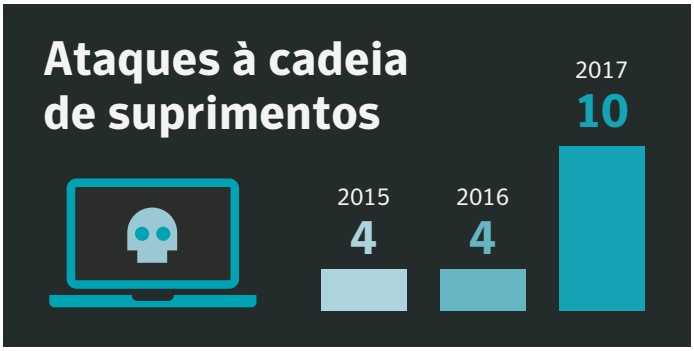
Explosão de ataques à mineração de criptomoedas

Cibercriminosos cujo foco era exclusivo em ransomware para geração de receita agora começam a explorar outras oportunidades. Durante o ano passado, a ascensão astronômica nos valores de criptomoedas inspirou muitos cibercriminosos a alterar seu foco para a mineração de moedas como uma fonte de receita alternativa. Essa corrida do ouro da mineração de criptomoedas resultou em um aumento de 8.500% nas detecções de mineradores de moedas em computadores de endpoints em 2017.



Com uma barreira reduzida de acesso – ao exigir apenas algumas linhas de código para operar – os cibercriminosos usam mineradores de moedas para roubar o poder de processamento do computador e o uso da CPU na nuvem de consumidores e empresas para minerar criptomoedas. Embora o impacto imediato da mineração de moedas seja tipicamente relacionado ao desempenho – lentidão de dispositivos, superaquecimento de baterias e, em alguns casos, inutilização de dispositivos – há implicações mais amplas, especialmente para as organizações. Redes corporativas estão em risco de paradas devido a mineradores de moedas.

À medida que a mineração maliciosa de criptomoedas evolui, os dispositivos de IoT continuarão sendo alvos maduros para exploração. A Symantec já identificou um aumento de 600% nos ataques globais de IoT em 2017, o que significa que os cibercriminosos poderiam explorar a natureza conectada desses dispositivos para mineração em massa.



Pico nos ataques à cadeia de suprimentos de software

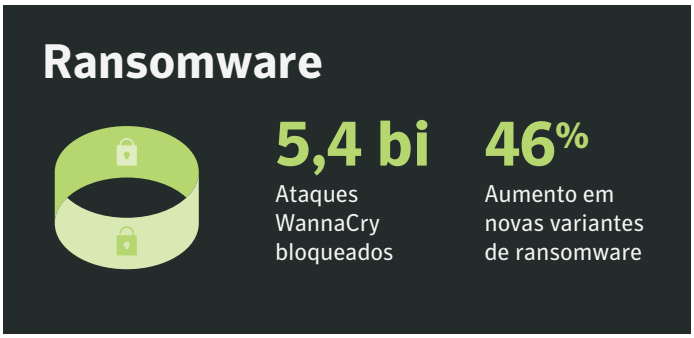
Apesar do exploit EternalBlue ter causado estragos em 2017, a realidade é que se torna cada vez mais difícil para os grupos de ataque identificarem e explorarem vulnerabilidades. Em resposta a este cenário, a Symantec agora observa um aumento em situações onde grupos de ataque injetam implantes de malware na cadeia de suprimentos para se infiltrar em organizações inocentes, com um aumento de 200% nesses ataques – um a cada mês de 2017 em comparação com quatro ataques anuais nos anos anteriores.

O sequestro de atualizações de software proporciona aos grupos de ataque um ponto de entrada para comprometer alvos bem protegidos ou para atingir uma região ou setor específico. O surto de Petya/NotPetya (Ransom.Petya) foi o exemplo mais notável: depois de explorar um software de contabilidade ucraniano como ponto de entrada, o Petya/NotPetya usou uma variedade de métodos, espalhando-se pelas redes corporativas para implantar a carga maliciosa dos grupos de ataque.

Negócios de ransomware enfrentam correção de mercado

Ao ser analisado como um negócio, fica claro que a rentabilidade do ransomware em 2016 gerou um mercado concorrido com demandas de resgate de valores exorbitantes. Em 2017, o "mercado" de ransomware sofreu uma correção com menos famílias de ransomware e demandas de resgate com valores mais baixos – sinalizando que o ransomware se tornou um commodity. Muitos cibercriminosos podem ter mudado seu foco para a mineração de moedas como uma alternativa para aproveitar os altos valores atuais das criptomoedas. Algumas ameaças a plataformas de banco online também reapareceram no mercado, devido a tentativa de diversificação de grupos de ransomware estabelecidos.

No ano passado, a demanda média de resgate caiu para US$ 522, menos da metade da média do ano anterior. E enquanto a quantidade de variantes de ransomware aumentou 46%, indicando que os grupos criminosos estabelecidos ainda continuam bastante produtivos, a quantidade de famílias de ransomware caiu. Estes números sugerem que os grupos estão inovando menos e podem ter mudado seu foco para novos alvos de maior valor.



A redução de instâncias de dia-zero não consegue impedir o aumento de ataques direcionados

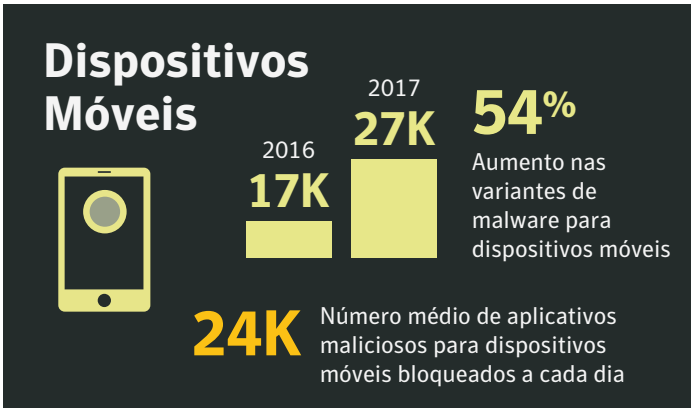
A Symantec identificou que o volume geral de ataques direcionados aumentou em 10% em 2017, motivado principalmente pela coleta de informações de inteligência (90%). No entanto, um número não tão insignificante de 10% dos grupos de ataque está envolvido em alguma forma de atividades disruptivas.

A tendência de "uso de ferramentas de dia-a-dia" continua, com grupos de ataque que optam por meios conhecidos e confiáveis para se infiltrarem em organizações estabelecidas como alvos.

Spear phishing é o vetor de infecção número um, empregado por 71% dos grupos organizados em 2017. O uso de ataques de dia-zero é cada vez menor. Na verdade, apenas 27% dos 140 grupos de ataques direcionados que são rastreados pela Symantec possuem histórico de utilização de vulnerabilidades de dia zero em algum momento no passado.

Aumento de instâncias de malware para dispositivos móveis

Ameaças no segmento de dispositivos móveis continuam a crescer a cada ano. A quantidade de novas variantes de malware para dispositivos móveis aumentou 54% em 2017, em comparação a 2016. E no ano passado, uma média de 24.000 aplicativos maliciosos para dispositivos móveis foram bloqueados a cada dia.



Além do aumento das ameaças, o problema é agravado pelo uso contínuo de sistemas operacionais desatualizados. Simplesmente, somente 20% dos dispositivos Android™ executam a versão principal mais recente e apenas 2,3% estão na última versão incremental.

Os usuários de dispositivos móveis também enfrentam riscos de privacidade gerados por aplicativos de grayware, que não são completamente mal-intencionados, mas podem ser problemáticos. A Symantec identificou que 63% dos aplicativos de grayware vazam o número de telefone do dispositivo. Com o aumento de grayware em 20% em 2017, este não é um problema que simplesmente desaparecerá.

Para mais detalhes, faça o download do

Relatório de Ameaças à Segurança na Internet Symantec 2018 (ISTR)

https://go.symantec.com/ISTR

Symantec

Sobre a Symantec

A Symantec Corporation (NASDAQ: SYMC) é líder mundial em soluções de cibersegurança e ajuda organizações, governos e indivíduos a proteger seus dados mais importantes onde quer que estejam. Organizações em todo o mundo buscam a Symantec para soluções estratégicas e integradas para se defender contra ataques sofisticados em endpoints, nuvem e infraestrutura.

Da mesma forma, uma comunidade global de mais de 50 milhões de pessoas e famílias dependem da suíte de produtos Norton e LifeLock da Symantec para proteger suas vidas digitais em casa e todos seus dispositivos. A Symantec opera uma das maiores redes civis de ciberinteligência do mundo, possibilitando a proteção contra as ameaças mais avançadas. Para mais informações, visite www.symantec.com ou conecte-se conosco no Facebook, Twitter, e LinkedIn.

Sede Mundial da Symantec
350 Ellis Street
Mountain View, CA 94043
United States of America

+1 650 527 8000
+1 800 721 3934

Para escritórios regionais e números de contato específicos, por favor visite nosso website. Para informações sobre o produto nos EUA, ligue gratuitamente para 1 (800) 745 6054.

Symantec.com

ISTR